UNITED STATES DISTRICT COURT

for the

District of Delaware

SEALED

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

information associated with [redacted]@icloud.com, [redacted]@brokennerd.com, [redacted]@ufso1.com, and [redacted]@icloud.com, that is stored at premises controlled by Apple Inc.

Case No. 23-75M

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

FILED

MAR - 3 2023

U.S. DISTRICT COURT DISTRICT OF DELAWARE

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252A(a)(2) and (a)(5)(b)	Distribution, Receipt and Possession of Child Pornography.

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Linh Phung
Applicant's signature

Linh Phung, Special Agent, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: 03/03/2023

Judge's signature

City and state: Wilmington, DE

Mary Pat Thynge, Chief U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Linh Phung, a Special Agent with the Federal Bureau of Investigation ("FBI"), Baltimore Division, Baltimore, Maryland, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts, "[redacted]**@icloud.com**" (TARGET ACCOUNT 1), "[redacted]**@brokennerd.com**" ("TARGET ACCOUNT 2"), "[redacted]**@ufso1.com**" (TARGET ACCOUNT 3), and "[redacted]**@icloud.com**" (TARGET ACCOUNT 4), (collectively, the "TARGET ACCOUNTS"), that is stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Infinite Loop, Cupertino, California.

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. I have been employed with the FBI as a Special Agent since May 2006. I am currently assigned to the Maryland Child Exploitation and Human Trafficking Task Force, which investigates individuals involved in the sexual exploitation of children. As part of my duties, I investigate crimes involving the sexual exploitation of minors, including sex trafficking, child pornography, and enticement violations.

4. Since being employed with the FBI, I have participated in the execution of numerous search warrants, including those for online accounts, such as email accounts, online storage accounts and other online communication accounts. In the course of employment with the FBI, I have observed and reviewed examples of child pornography (as defined in 18 U.S.C. § 2256) in many forms of media.

5. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States

6. In this Affidavit, I set forth facts to show that there are sufficient grounds to find probable cause to believe that beginning in or about August 2021, MICHAEL NATALE ("NATALE") committed violations of the following: Title 18, United States Code, Section 2252A(a)(2) (distribution and receipt of child pornography) and Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography) (hereinafter referred to as the "TARGET OFFENSES"). There is also probable cause to believe that the TARGET ACCOUNTS contain evidence of the TARGET OFFENSES, and thus probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

7. The statements in this affidavit are based in part on information and reports provided by the FBI and other law enforcement, and on my experience and background as a Special Agent of the FBI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of the TARGET OFFENSES are located within the TARGET

ACCOUNTS. I have not, however, withheld any fact necessary to a determination of probable cause.

8. Unless otherwise stated, the conclusions and beliefs I express in this affidavit are based on my training, experience, and knowledge of the investigation, and reasonable inferences I've drawn from my training, experience, and knowledge of the investigation.

JURISDICTION

9. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

SPECIFIED FEDERAL OFFENSES

10. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Section 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any mean, including by computer.

b. Title 18, United States Code, Section 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any mean, including by computer.

DEFINITIONS

11. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short

in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

c. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

d. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image of picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, tablets, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

f. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

g. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which

perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

j. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

k. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

l. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

m. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

n. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

o. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c)

masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

p. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

q. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO POSSESS AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND THE INTERNET RELATES TO THE POSSESSION, RECEIPT AND DISTRIBUTION OF CHILD PORNOGRAPHY

12. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the internet to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children

typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or cellphone, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer to Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

13. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required

significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers, smartphones and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers, smartphones and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a computer (via a USB cable) or connect with a computer via Bluetooth, and transfer data files from one digital device to another. Some "smartphone" users can and do create, communicate, upload, and download child pornography, and communicate with children to coerce them or entice them to produce child pornography or perform sexual acts, by using internet based social media or electronic service providers like Instagram, Snapchat, or Apple (and many others).

d. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo, and Google LLC, Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers, and is occasionally retained by the providers after the user deletes the data from their account.

f. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

g. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and the increased storage capacity of computers and server space over time, there exists a fair probability that evidence regarding the distribution, receipt and possession of child pornography will be found in the TARGET ACCOUNTS notwithstanding the passage of time.

KIK

14. Kik is a free instant messenger application for mobile devices in which users can send text messages, pictures, and videos to other users. Users can communicate directly with an individual or with multiple users in a group chat. When signing up for a Kik account, a user supplies an email address (which does not need to be verified), a unique username, and a display name that is seen when chatting with others. Kik may retain images and video content sent and received by users for approximately 30 days. Kik may also retain a log of all the messages that a user has sent and received, including senders' and receivers' usernames; however, the log does not include the actual message that was sent. The text of the chat messages sent may be stored locally on the user's devices.

PROBABLE CAUSE

15. On or about August 27, 2021, FBI Newark received information from FBI Milwaukee that an online undercover employee (hereinafter the "UC") joined a private group on the Kik messenger application called "Joe's Basement." The UC communicated with one of the administrators of the private group, who utilized the Kik display name "Dominique." The private group was known to the UC as a group where people meet to discuss and exchange sexually explicit images/videos of children. "Dominique" told the UC that she had a four-year-old son she was sexually active with. "Dominique" sent the UC approximately five files depicting child pornography, as defined in 18 U.S.C. § 2256. When the UC asked Dominique how far she got with her son, "Dominique" provided the following response:

> "Ive sucked him while he was asleep. He got hard tho. And ive tried to put him inside me BUT hed always wake up and push me off. So I stop. I really don't wanna mess with it while hes awake because I don't trust he won't say something especially to his dad."

16. "Dominique" was identified by FBI Newark and on or about August 31, 2021, she was arrested for production, distribution and advertisement of child pornography.

17. On or about November 3, 2021, federal search warrants were issued for the Kik group "Joe's Basement" and for the Kik account associated with "Dominique."

18. In February 2022, FBI Newark reviewed the search warrant results provided by Kik and observed that "Dominque" communicated with another Kik username, "nottelling733." Specifically, "Dominique" sent "nottelling733" approximately 12 videos and one image file depicting child pornography. Your affiant reviewed the files, two of which are described as follows:

a. **File ending in "2c33f53df697.jpg"** – Image depicted a nude prepubescent boy with the focus on his penis. FBI Newark identified this boy as Dominique's son.

b. **File ending in "44a6fdcbc9db"** – Video length is approximately 43 seconds depicted what appeared to be a male penetrating the anus of a prepubescent infant/toddler boy.

19. "Nottelling733" also sent approximately six video files and one image file depicting child pornography to Dominique between approximately August 22, 2021 and August 25, 2021. Your affiant reviewed the files, three of which are described as follows:

a. **File ending in "c880d0bc3436"** – Video length is approximately 31 seconds and depicted what appeared to be a woman bending over a prepubescent boy while the boy's anus being penetrated by an unidentified male.

b. **File ending in "a4ceac9bf649"** – Video length is approximately 38 seconds and depicted a nude prepubescent boy with his legs spread apart. An erect penis penetrated the boy's anus and then the unidentified individual ejaculated on the boy.

c. **File ending in "7866b3e8d4e4"** – Video length is approximately one minute and 48 seconds. Video depicted two parts. In the first half of the video, there was unidentified individual shoving his penis into the infant's mouth. The infant appeared to be crying. In the second half of the video, there appeared to be a nude infant on a boppy on the couch. An unidentified individual shoved his penis into the infant's mouth.

20. Kik further provided a report that noted the source of the files exchanged between Dominique and "nottelling733." According to the report, "nottelling733" sent the files from their "Gallery" app. Based on training and experience, I know that "gallery" is also known as the "Photos"

application on a cellular device, to include Android and iPhone devices.

21. In March 2022, additional records were obtained from Kik for the account associated with username "nottelling733." Kik provided that the email associated with the account was "olivebranch733@gmail.com;" that the device type was "iphone"; and that one of the IP addresses associated with the account was 174.198.212.125. [1]

22. In May 2022, as the investigation continued, records were obtained from Verizon for the aforementioned IP address within the timeframe provided by Kik. Verizon provided that the IP address was connected to telephone number [redacted], and that the telephone number was subscribed to NATALE at [redacted] Laurel, Delaware 19956.

23. Database checks revealed that NATALE was arrested on August 1, 2019 by the Delaware State Police for possession of child pornography. NATALE was ultimately convicted and required to register as a sex offender. He was sentenced to two years' probation, which began around May 2021.

24. The Kik returns also showed that "Nottelling733" sent a photograph of himself to "Dominique" – a photograph that was similar to the driver's license picture for NATALE, as well as to NATALE's mugshot. Also in the photograph sent by "nottelling733," your affiant observed what appeared to be a tattoo on his chest. The tattoo matches the tattoo description in the law enforcement database checks for NATALE.

25. In December 2022, FBI Baltimore received the information about NATALE from FBI Newark. Upon receipt and review of the information provided by FBI Newark, FBI Baltimore notified Delaware Probation and Parole (hereinafter "DPP") of NATALE's August 2021 activity.

26. DPP confirmed that NATALE had been residing at 125 Brooklyn Avenue, Laurel,

[1] The IP address provided is a Natting IP router, which can have many users at one time. Therefore, a specific port number was provided to narrow down the user. In this case, the port number was 11464 based on the Natting IP address spreadsheet provided by Verizon.

Delaware 19956 since May 2021, and that the telephone number DPP had for NATALE was [redacted]. This matches the information provided by Verizon based on the IP address from the Kik return for "nottelling733." DPP also informed your affiant that NATALE currently has a girlfriend who has an 11-year-old daughter and a six-year-old autistic son.

27. In January 2023, unbeknownst to your affiant, DPP checked NATALE's phone and did not observe any files depicting child pornography on the phone itself. DPP did not learn the type of phone NATALE had or how long NATALE had the phone.

28. In or around February 2023, your affiant obtained records from Apple for any accounts associated with NATALE by way of address and phone number. Apple provided TARGET ACCOUNTS 1-3. Notably, Apple provided that each of these Target Accounts utilizes the iCloud feature for photos. TARGET ACCOUNT 3, in particular, indicated significant iCloud activity. TARGET ACCOUNT 4 was listed for TARGET ACCOUNT 3 under the "Hide My Email"[2] feature.

BACKGROUND CONCERNING APPLE[3]

29. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

30. Apple provides a variety of services that can be accessed from Apple devices or, in some

[2] "Hide My Email" is an Apple feature that generates unique, random email addresses that automatically forward to your personal inbox. Each address is unique to you. You can read and respond directly to emails sent to these addresses all while your personal email address is kept private.

[3] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include instant messaging, photo storage, and other file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

e. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

f. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

31. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, Photos, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

32. Apple captures information associated with the creation and use of an Apple ID. During

the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

33. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

34. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's web browser may be captured when used to access services through

icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

35. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

36. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element.

37. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a

residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

38. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation, such as images depicting child pornography contained in the photos section or in attachments to e-mails the user is sending to others or to himself. Especially in the case of individuals with a sexual interest in children, who are known to collect and retain images and videos containing visual depictions of minors engaged in sexual activity for many years. The stored data may also provide indirect evidence of the offenses under investigation, such as the timeline of the offenses. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

39. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators or victims, as well as

instrumentalities of the crimes under investigation.

40. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

41. Based on the foregoing, I request that the Court issue the proposed search warrant.

42. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, good cause exists to permit the execution of the requested warrant at any time in the day or night.

/s/ Linh Phung
Special Agent Linh Phung
Federal Bureau of Investigation

Sworn to me over the telephone and signed by me pursuant to
Fed. R. Crim. P. 4.1 on this 3 day of March, 2023.

HONORABLE MARY PAT THYNGE
CHIEF UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with "[redacted]**@icloud.com**", "[redacted]**@brokennerd.com**", "[redacted]**@ufso1.com**", and "[redacted]**@icloud.com**" (collectively, the "TARGET ACCOUNTS), that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Infinite Loop, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by Apple, Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on February 7, 2023[4], Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber

[4] ID number 20230016559.

Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account from June 1, 2021 through the present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from June 1, 2021 through the present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and

query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of the TARGET OFFENSES listed in the Affidavit, those violations involving NATALE, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Any and all notes, documents, records, or correspondence pertaining to child pornography, as defined in 18 U.S.C. § 2256(8);

(b) Any and all correspondence identifying persons producing, transmitting, receiving or possessing any child pornography;

(c) Any and all records reflecting personal contact and any other activities with minors;

(d) Any and all financial documents, records, receipts, credit card statements, and/or correspondence relating to payments sent and/or received in connection with minors engaged in sexually explicit conduct, nude pictures, modeling, and/or hosting websites, including any PayPal, CashApp, or Venmo records;

(e) Any and all notes, documents, records, photos or correspondence that indicate a sexual interest in children, including, but not limited to Internet browsing history;

(f) Any and all visual depictions of minors, to include depictions of minors engaged in sexually explicit conduct, nude pictures, and modeling;

(g) All images, messages, and communications regarding methods to avoid detection by law enforcement;

(h) Any and all records pertaining to Kik activity;

(i) All "address books" or other lists of contacts;

(j) Evidence indicating the account owner's state of mind as it relates to the events set forth in the Affidavit;

(k) The identity of the person(s) who communicated with the user ID about matters relating to the TARGET OFFENSES listed in the Affidavit, including records that help reveal their whereabouts;

(l) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH [redacted]**@icloud.com,** [redacted]**@brokennerd.com,** [redacted]**@ufso1.com,** and [redacted]**@icloud.com** THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	Case No. 23- **Filed Under Seal**

APPLICATION FOR ORDER COMMANDING APPLE INC.
NOT TO NOTIFY ANY PERSON OF THE EXISTENCE OF SEARCH WARRANT

The United States requests that the Court order Apple Inc ("Apple") not to notify any person (including the subscribers or customers of the account(s) listed in the warrant) of the existence of the attached search warrant until six months from the date of the attached Order.

Apple is a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(2). Pursuant to 18 U.S.C. § 2703, the United States obtained the attached search warrant, which requires Apple to disclose certain records and information to the United States. This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." *Id.*

In this case, such an order would be appropriate because the attached warrant relates to an ongoing criminal investigation into child pornography offenses. Much of the evidence in this investigation is electronically stored. Notifying the target of the instant warrant would give the target an opportunity to destroy or tamper with evidence, change patterns of behavior, or intimidate

potential witnesses, which would seriously jeopardize the investigation or unduly delay a trial. *See* 18 U.S.C. § 2705(b).

WHEREFORE, the United States respectfully requests that the Court grant the attached Order directing Apple not to disclose the existence or content of the attached search warrant for six months from the date of the attached Order, except that Apple may disclose the attached warrant to an attorney for Apple for the purpose of receiving legal advice.

The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Executed on March 2, 2023.

/s/ Briana Knox
Briana Knox
Assistant U.S. Attorney

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH [redacted]**@icloud.com,** [redacted]**@brokennerd.com,** [redacted]**@ufso1.com,** and [redacted]**@icloud.com** THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	Case No. 23- **Filed Under Seal**

ORDER

The United States has submitted an application pursuant to 18 U.S.C. § 2705(b), requesting that the Court issue an Order commanding Apple Inc. ("Apple"), an electronic communication service provider and/or a remote computing service, not to notify any person (including the subscribers or customers of the account(s) listed in the warrant) of the existence of the attached search warrant until six months from the date of this Order.

The Court determines that there is reason to believe that notification of the existence of the attached warrant will seriously jeopardize the investigation, including by giving the target an opportunity to destroy or tamper with evidence, change patterns of behavior, or intimidate potential witnesses. *See* 18 U.S.C. § 2705(b).

IT IS THEREFORE ORDERED under 18 U.S.C. § 2705(b) that Apple shall not disclose the existence of the attached search warrant, or this Order of the Court, to the listed subscriber or to any other person, for a period of six months from the date of this Order, except that Apple may disclose the attached subpoena to an attorney for Apple for the purpose of receiving legal advice.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court.

3/3/2023
Date

Chief United States Magistrate Judge